

# Chapter 5: Accessing Kerberized Machines



In this chapter we discuss accessing systems in the FNAL.GOV realm from UNIX, Windows and Macintosh machines. We cover logging in at the console, connecting over the network, and using portal mode.

Very important note: Any time you're about to enter your Kerberos password, first verify that you're using an encrypted connection or using the host's directly-connected keyboard! Otherwise you risk exposing your password. See Appendix A: *Encrypted vs. Unencrypted Connections* for information.

## 5.1 Trying Out Kerberos on fnkerb.fnal.gov

---

As of July 2, 2001, the Computing Division has set up a Kerberized Linux system in the FNAL.GOV strengthened realm for use by all Fermilab employees and users, local and remote, to change passwords and test basic Kerberos functionality. The machine name is fnkerb.fnal.gov, and it is accessible to everyone who has both a Kerberos principal and an account on fnalu. The fnkerb system is configured to use AFS as a login area. It is configured to allow the following access methods:

- non-Kerberized ssh with your AFS password (see section 5.9 *Logging In from Off-Site*)
- Portal mode via CRYPTOCARD (see section 5.5 *Connecting from a NonKerberized Machine: Portal Mode*).
- Kerberos via Kerberized versions of **telnet**, **ftp**, **rsh**, **rlogin**, and **rcp** (see sections 5.3 *Connecting from One Kerberized Machine to Another*, 5.6 *Logging In Through WRQ® Reflection Software from a PC*, 5.8 *Logging In from a Macintosh*)

Please note the following:

- Fnkerb has a limited lifetime; it will be shutdown on December 18, 2001.
- We ask that you limit your activities on fnkerb to acquainting yourself with Kerberos. The system is not configured to support general user activities (e.g., web browsing, reading email) or physics analysis. No batch facilities, CVS repositories, etc., are available.

- All questions about Kerberos and its use on this system should be directed to *helpdesk@fnal.gov* or *kerberos-users@fnal.gov*.
- Issues with the operating system on fnkerb should be reported to *helpdesk@fnal.gov*.
- Support on fnkerb is available Monday through Friday, 9:00 to 5:00.

## 5.2 Logging In at the Console of a Kerberized UNIX Machine

---



Note that if you have an account and a standard UNIX password (in the `passwd` file or NIS map) but no principal or Kerberos password, you can log in at the console and use non-Kerberized services. (From any terminal other than the console, the Kerberized machine responds in portal mode and you have no option to enter your UNIX password.) The rest of this chapter (and really, the rest of the manual!) assumes that you have a principal and Kerberos password.

### 5.2.1 Using Standard UNIX Login Program



If you are running the standard login program, log in at the console normally, entering your standard UNIX password (note that if your machine runs AFS, your UNIX and AFS passwords may be the same). The standard login program does not accept your **kerberos** password. You need to run **kinit** after logging in to obtain your credentials. The credentials should then get forwarded to other strengthened machines normally. The **kerberos** login program is not installed by default with the **kerberos** product.

### 5.2.2 Using Kerberos Login Program

If your machine is configured to use the **kerberos** login program<sup>1</sup>, enter your Kerberos password when you log in. You should not need to run **kinit** after login. (You can still login using your UNIX password, then run **kinit** to get Kerberos tickets, if you wish.) An advantage to using the **kerberos** login program is that it checks the `/etc/krb5.conf` file in which you or your system administrator can set defaults for Kerberized applications.

---

1. Not applicable to IRIX systems or to Linux, or to Solaris if using the GUI login box. The login program isn't run in these cases.

## 5.3 Connecting from One Kerberized Machine to Another

---

Make sure you have credentials on the source machine, then run the Kerberized version of the connection program you want to use (e.g., **ssh**, **slogin**, **telnet**, **rsh**, **rlogin**, **rcp**, **scp** or **FTP**). The Kerberized features of these programs are described in Appendix D: *Network Programs Available on Kerberized Machines*. Assuming your credentials get forwarded to the target machine, you should be automatically recognized and authenticated there; you should not be prompted for your Kerberos password.

A couple of notes:

- Depending on the login program that the target machine runs, you may be able to log in using your UNIX password, as described above in section 5.2 *Logging In at the Console of a Kerberized UNIX Machine*. After logging in, you will need to run **kinit** to authenticate to Kerberos in this case.
- If the usernames on the machines differ, use the **-l** `<target_host_login_name>` option.
- If ticket forwarding has been set “off” for your system, and you want to connect to a Kerberized machine with ticket forwarding turned on, use the **-f** or **-F** option (for **telnet**, **rsh**, **rlogin**). **-F** marks them reforwardable. Forwarding is described in section 6.2.4 *Forwarding Tickets*.
- If ticket forwarding has been set “on” for your system, and you want to connect to a Kerberized machine with ticket forwarding turned off, use **the -N** option (for **telnet**, **rsh**, **rlogin**, **rcp**), or **-k** for Kerberized **ssh**. Forwarding is described in section 6.2.4 *Forwarding Tickets*.



Warning! If your on-site Kerberized system accepts a reusable login password over the network (even on an encrypted connection), this is a violation of the Fermilab Policy on Computing (see <http://www.fnal.gov/cd/main/cpolicy.html>).

## 5.4 Connecting from a Machine Running Kerberized SSH

---



Any machines that are sited at FNAL and that wish to use ssh will be required to use Kerberized ssh (available from `ftp://ftp.fnal.gov/KITS/` as `ssh v1_2_27` or higher). Non-kerberized ssh is not permitted on these machines.

With both **kerberos** and Kerberized **ssh** installed on your machine, make sure you have a Kerberos ticket, then run the Kerberized version of the connection program you want to use (e.g., **ssh**, **slogin**, or **scp**) to connect to a remote Kerberized host. The Kerberized options for these programs are described in Appendix D: *Network Programs Available on Kerberized Machines*. You do not get prompted for your Kerberos password during login.

**Ssh** encrypts the connection by default typically (check your configuration). You can always use the **-c <cipher>** option to ensure encryption.

## 5.5 Connecting from a NonKerberized Machine: Portal Mode

---

### 5.5.1 About Portal Mode

At Fermilab, strengthened machines are configured to respond in *portal mode* when requests for access come from machines outside the trusted realm<sup>1</sup>. In portal mode, the Kerberized machine acts as a secure gateway into the strengthened realm, requiring a single-use password for authentication. This avoids transmission of reusable clear-text passwords over a potentially unprotected network. The non-reusable authentication method for portal mode that the Computing Division currently supports is CRYPTOCARD.

Once you've logged on successfully through the portal, the KDC "knows who you are", and the machine obtains your Kerberos credentials for you. From a given strengthened machine, you should not be required to provide your Kerberos password when accessing other machines in Fermilab's strengthened realm. **In particular, never enter your Kerberos password when using an unencrypted connection!** (See Appendix A: *Encrypted vs. Unencrypted Connections*.)

---

1. From a trusted realm, if credentials don't grant you access to your account

## 5.5.2 About CRYPTOCard

Fermilab is implementing portal mode using CRYPTOCard technology. A CRYPTOCard is a calculator-style, battery-powered device used for generating a single-use password.



To read more about what a CRYPTOCard is and how it works, see Appendix B: *Getting Started with your CRYPTOCard*. To request one (or CRYPTOCard software for Palm Pilot -- not currently available), fill out the online form *Form to Request Kerberos Principal and/or Related Items* at <http://www.fnal.gov/cd/forms/strongauth.html>. When you get your CRYPTOCard, go back to Appendix B for information on how to use it and take care of it.



Two notes:

- No special hardware or software is required on the nonKerberized machine for CRYPTOCard use.
- The CRYPTOCard login code assumes that the user's login name and principal match. If yours don't match, you won't be able to log in using this method.

## 5.5.3 Programs for Initiating CRYPTOCard Login

To log on to a machine in the FNAL.GOV realm from your nonKerberized machine, run any of the following commands:

```
% ssh <host>
% slogin <host>
% telnet <host>
% ftp <host>
```

as usual (the standard, nonKerberized version of the program, as the Kerberized version is not available on nonKerberized machines).

Regarding the use of **ssh** and **slogin**, the CRYPTOCard login program supports **ssh** only when no command argument is given, i.e., when it is effectively equivalent to **slogin**. Fundamentally, the only **ssh** program supported is **slogin**. Note that it is necessary to give an empty password to **ssh** in order to get the CRYPTOCard challenge.

After you issue the network command, the remote host will prompt you to provide a non-reusable password rather than your Kerberos password:

Press ENTER and compare this challenge to the one on your display: [12345678]

Enter the displayed response:

Use your CRYPTOCARD to provide this password, as described in section B.4 *Log in Using CRYPTOCARD (the First Time)*, section B.5 *Log in Using CRYPTOCARD (Normally)*, or briefly in section 5.5.4 *Summary of the “Normal” Login Steps with CRYPTOCARD*.



Notes:

- Never type your Kerberos password over a CRYPTOCARD **telnet** session! The connection is not encrypted.
- You may safely type your password over an encrypted CRYPTOCARD **ssh/slogin** session.
- **rsh**, **rlogin**, **rcp** and **scp** are not available for portal mode.

## 5.5.4 Summary of the “Normal” Login Steps with CRYPTOCARD

The full description of using a CRYPTOCARD is given in Appendix B: *Getting Started with your CRYPTOCARD*. Assuming you’ve read that, this is just a reminder!

- 1) CRYPTOCARD: **ON**, [**PIN**], **ENT**, **ENT**, **ENT**
- 2) Host: Run **telnet <hostname>** or **ftp <hostname>** and provide your principal.
- 3) Host: type response, press **RETURN**
- 4) CRYPTOCARD: **OFF**

If you want to generate another response before turning it off, just press **ENT** again three times (once to get past the Fermilab id, once to display the next challenge, and once to display the response).

## 5.5.5 Portal Mode FTP when you can’t see the Challenge

If you’re doing portal mode **FTP** with a client that does not show you the output text from the server (e.g., **FTP** under **emacs**), it won’t display the challenge string. In this case, go ahead and use your CRYPTOCARD anyway, and enter the response as your password. This works if your card is in sync with the KDC, which should generally be the case.

If the **FTP** login is unsuccessful, you need to synchronize your card. To do so, start a **telnet** connection, and type the displayed challenge into your CRYPTOCARD. Then disconnect the **telnet** session BEFORE you enter the response so that you save it for your **FTP** session! Otherwise the response will get used and you'll be out of sync again.

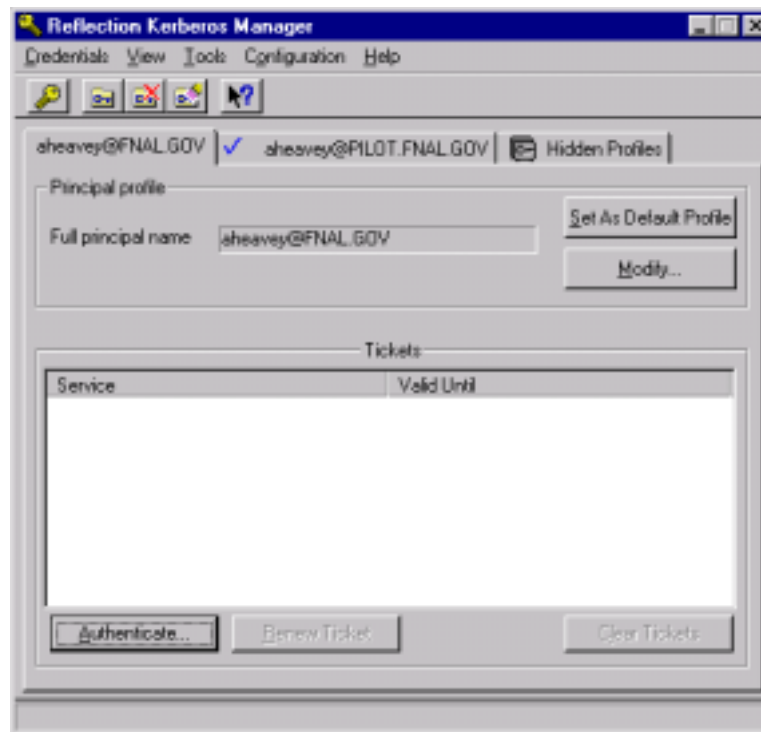
## 5.6 Logging In Through WRQ® Reflection Software from a PC

---

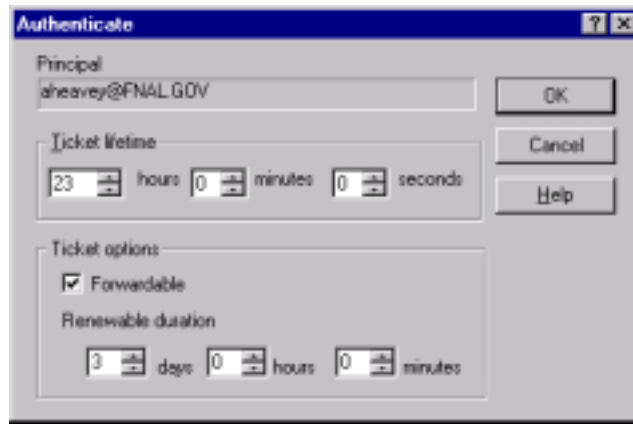
### 5.6.1 Preauthenticate via the Kerberos Manager (Optional)

The **Reflection Kerberos Manager** program preauthenticates you to Kerberos. This means it obtains Kerberos tickets for you according to the principal you choose (you may have one for PILOT.FNAL.GOV and for FNAL.GOV), and you can freely connect to machines in the corresponding realm without needing to type your Kerberos password each time.

Navigate to **START > PROGRAMS > REFLECTION > UTILITIES > KERBEROS MANAGER** to open the **Reflection Kerberos Manager** application.



Choose your principal that corresponds to the default realm of the target machine. Click **AUTHENTICATE**.



- Verify or change **TICKET LIFETIME** (if you give a value greater than the KDC limit of 23 hours, the renewable lifetime will be set to 23 hours)
- Check **FORWARDABLE** if you want your tickets forwarded to target host (you need a forwardable ticket to have an AFS ticket automatically generated when you connect to a system)
- To set your ticket as renewable, enter a non-zero time for **RENEWABLE DURATION** (if you give a value greater than the KDC limit of seven days, the renewable lifetime will be set to seven days)

Click **OK**, and provide your Kerberos password at the prompt. Back on the **KERBEROS MANAGER** window, you should see (at least) the new ticket-granting ticket (TGT) `krbtgt/FNAL.GOV@FNAL.GOV`. (older graphic, but it shows the tickets)

If you receive an error message instead, check that the above steps were followed correctly and that you typed the right password. If you continue to receive an error message, send the exact error message text to `nightwatch@fnal.gov`.



Once you run **Reflection Kerberos Manager** and authenticate, you do not need to keep the application active; you can exit out and continue to log in to Kerberized machines. The authentication is valid for the lifetime of the ticket.



When you have finished your session and disconnected from all Kerberized machines, it's important to prevent another user at your machine from using your tickets. Bring up the application again and clear your tickets by clicking **CLEAR TICKETS** on the **REFLECTION KERBEROS MANAGER** window. You can automate this by clicking **CLEAR ALL TICKETS ON SHUTDOWN** on the **CONFIGURATION** menu.

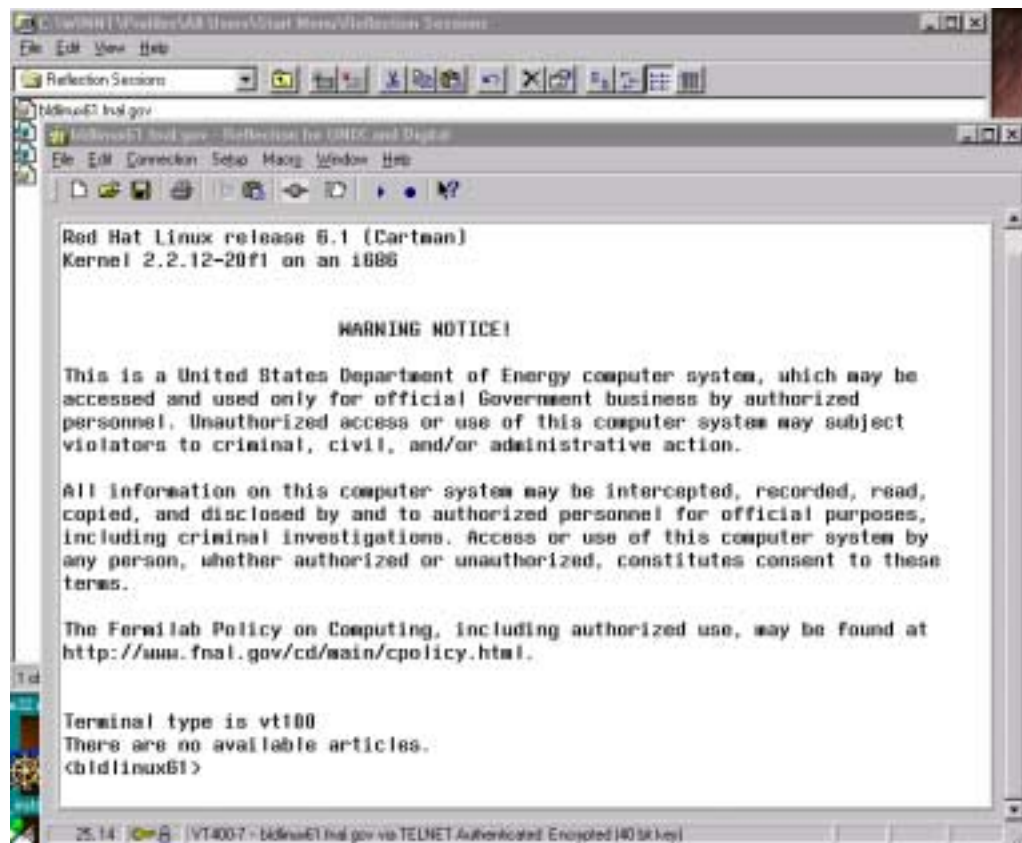


## 5.6.2 Run a telnet Session to Kerberized Host

To use the **WRQ® Reflection telnet** client to access machines in the strengthened realm, you need to set (and save) a separate **telnet** configuration for each host. This procedure is outlined in section 12.8 *Configuring WRQ® Reflection telnet Connections*. Each saved configuration is maintained as a file in your **REFLECTION** folder (set as the User folder in section 12.5 *Installing WRQ® Reflection Security Components v8.0.0*), its default filename corresponding to the host name.

You can choose to start the **Reflection Kerberos Manager** first to preauthenticate, as explained in section 5.6.1 *Preauthenticate via the Kerberos Manager (Optional)*. To start your session:

- Navigate to **START > PROGRAMS > REFLECTION > HOST - UNIX AND DIGITAL**.
- On the **REFLECTION FOR UNIX AND DIGITAL** window, select **FILE > OPEN**.
- Double click on the file in your **REFLECTION** folder corresponding to the host to which you want to connect. (If you haven't preauthenticated you will be prompted to provide your Kerberos password.) It will bring up a VT window and log you in:



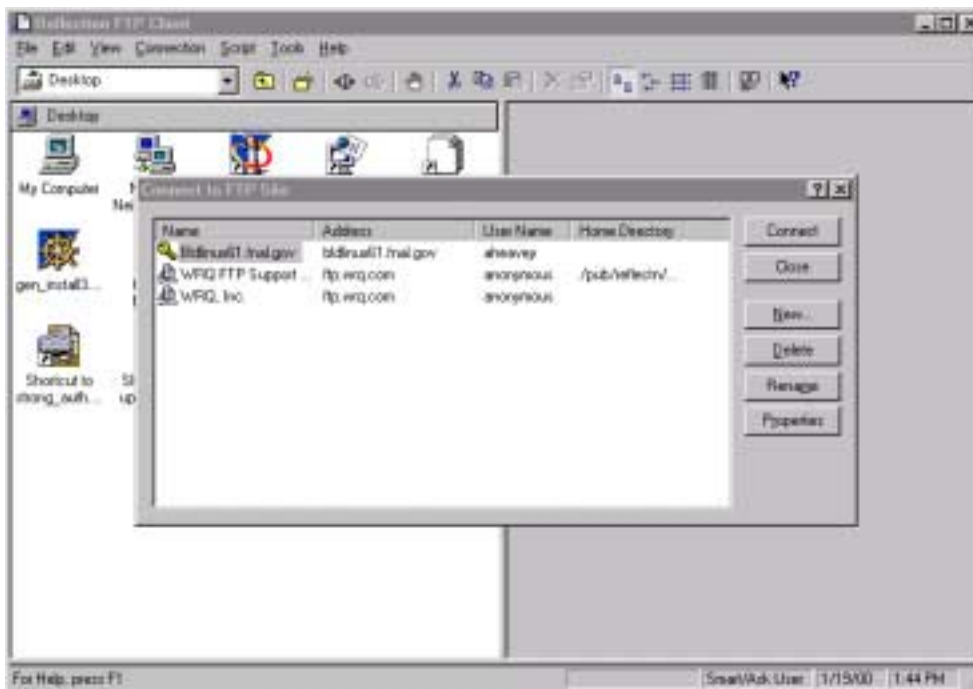
If you have preauthenticated with a forwardable ticket, and/or if your telnet configuration file specifies `Forward ticket`, then you have credentials on the host (including AFS token if needed).

If you did not log in with a forwardable ticket, then to obtain credentials on the host (and to obtain an AFS token if AFS runs on the host) you will need to run **kinit** (see section 6.2.1 *Obtaining Tickets*) and enter your password again after you log in. *Before* you enter your password, glance at the bottom of the VT window and verify that it says “Encrypted” and shows a locked lock icon (as shown on the above image). If it doesn’t, *log out and verify your configuration* (under **CONNECTION>SECURITY**, check **Reflection Kerberos** and check **Encrypt data stream**)! **Always make sure the data stream is encrypted before entering your password!**

### 5.6.3 Run an FTP Session to Kerberized Host

Configuration of **FTP** sessions is covered in section 12.9 *Configuring WRQ® Reflection FTP Connections*. Make sure that the default realm for **REFLECTION** is set to the default realm of the target host (see number [3] in section 12.6 *Configuring WRQ® Reflection Security Components v8.0.0*).

To use the **Reflection FTP** client to access a Kerberos system: open **START > PROGRAMS > REFLECTION > FTP CLIENT**:



and double-click the file corresponding to the host you want to access.

## 5.7 Logging In Through Kerberized Exceed 7 Software from Windows

---

You should create one secure telnet profile for each Kerberized host you wish to access, according to the instructions in section 13.5 *Configuring the Exceed 7 Telnet Application*. To preauthenticate:

- using the **Leash32** utility, navigate to **START > PROGRAMS > KERBEROS UTILITIES > LEASH32**. Select **GET TICKET** on the **ACTION** menu.

You will be required to enter your Kerberos password. Ignore the CRYPTOCARD prompt that may follow (press **CANCEL**). Your ticket will appear in the **Leash32** window. Click on the Windows Explorer-style plus signs (+) to get details.

- using the command prompt, type **kinit -5** to request a ticket.

You will be required to enter your Kerberos password. Ignore the CRYPTOCARD prompt that may follow (just press **ENTER**). To verify the ticket and its flags, either bring up the **Leash32** window, or type **klist -f** at the command prompt.

To connect:

- 1) Start the Exceed 7 telnet program. Navigate to **START > PROGRAMS > HUMMINGBIRD CONNECTIVITY v7.0 > HOSTEXPLORER > TELNET**.
- 2) On the **OPEN SESSION** window, with the desired telnet profile selected, the target host name or IP address should appear in the Host Name window. To connect, click on the **CONNECT** button. If you've preauthenticated, you should get right in without having to provide your Kerberos password.
- 3) The **LEASH32** window should now show your host connection in addition to the kerberos ticket.

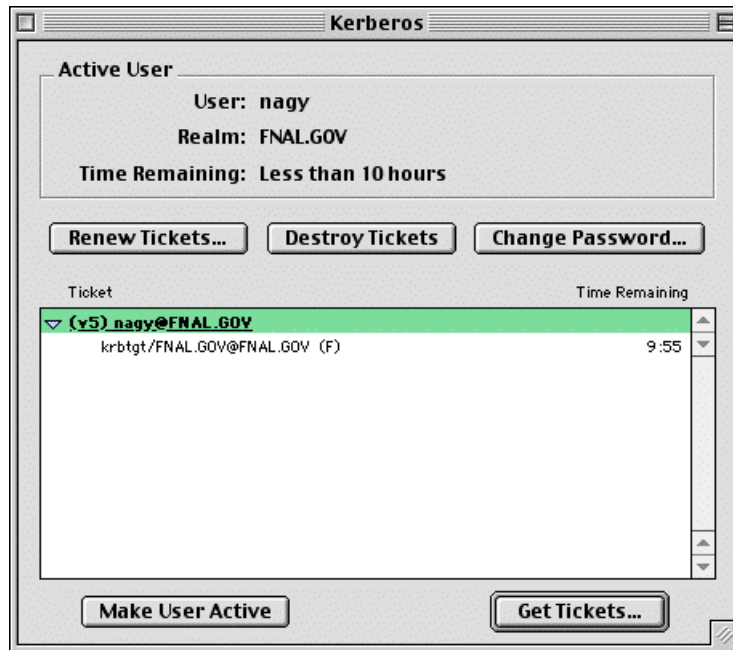
## 5.8 Logging In from a Macintosh

---

Here we assume you are running the **MIT Kerberos** software for Macintosh as described in Chapter 15: *Installing and Configuring MIT Kerberos on a Macintosh System*.

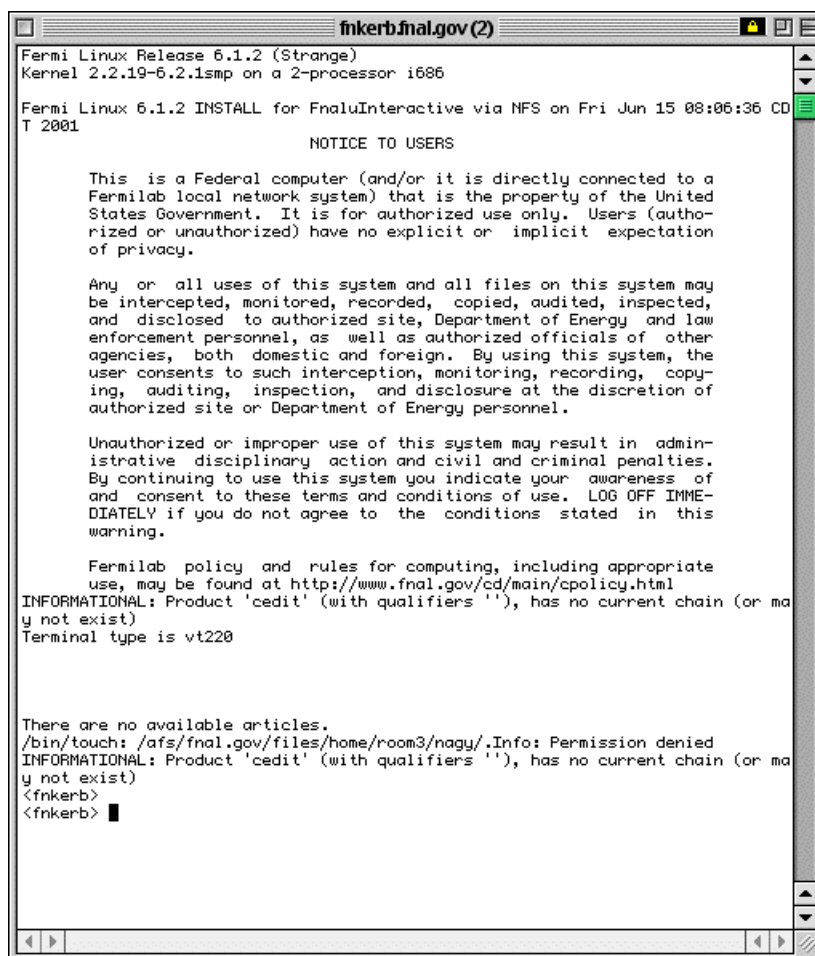
## 5.8.1 Authenticate via Kerberos Control Panel

- Invoke the **Kerberos Control Panel** (from **CONTROL PANELS** under the Apple menu, from the **KERBEROS MENU** in the menu bar, or from the **KERBEROS CONTROL STRIP** module).



- Select principal, and click **GET TICKETS**.
- Enter your Kerberos password on the pop-up screen.

You should see a ticket appear. Now you can invoke your **telnet** product (**BetterTelnet** or **NiftyTelnet**) and connect to one or more strengthened hosts without having to provide your password again.



```
fnkerbfnal.gov (2)
Fermilab Linux Release 6.1.2 (Strange)
Kernel 2.2.19-6.2.1smp on a 2-processor i686

Fermilab Linux 6.1.2 INSTALL for FnalInteractive via NFS on Fri Jun 15 08:06:36 CD
T 2001

NOTICE TO USERS

This is a Federal computer (and/or it is directly connected to a
Fermilab local network system) that is the property of the United
States Government. It is for authorized use only. Users (author-
ized or unauthorized) have no explicit or implicit expectation
of privacy.

Any or all uses of this system and all files on this system may
be intercepted, monitored, recorded, copied, audited, inspected,
and disclosed to authorized site, Department of Energy and law
enforcement personnel, as well as authorized officials of other
agencies, both domestic and foreign. By using this system, the
user consents to such interception, monitoring, recording, copy-
ing, auditing, inspection, and disclosure at the discretion of
authorized site or Department of Energy personnel.

Unauthorized or improper use of this system may result in admin-
istrative disciplinary action and civil and criminal penalties.
By continuing to use this system you indicate your awareness of
and consent to these terms and conditions of use. LOG OFF IMME-
DIATELY if you do not agree to the conditions stated in this
warning.

Fermilab policy and rules for computing, including appropriate
use, may be found at http://www.fnal.gov/cd/main/cpolicy.html
INFORMATIONAL: Product 'cedit' (with qualifiers ''), has no current chain (or ma
y not exist)
Terminal type is vt220

There are no available articles.
/bin/touch: /afs/fnal.gov/files/home/room3/nagy/.Info: Permission denied
INFORMATIONAL: Product 'cedit' (with qualifiers ''), has no current chain (or ma
y not exist)
<fnkerb>
<fnkerb> █
```

## 5.8.2 Authenticate at Login

Invoke **BetterTelnet** or **NiftyTelnet** and connect to a strengthened host. You will be prompted for your Kerberos password, and then authenticated once you have provided it.

## 5.9 Logging In from Off-Site

Due to practical considerations, namely the fact that off-site machines at universities may be shared by many people, some of whom do not access Fermilab at all, off-site users are not required to install a Kerberos 5 client.

Off-site machines may access Fermilab's Kerberized systems using ssh with passwords, public/private keys, host-based keys or Kerberos on their machines at their university or home.

## 5.9.1 Description of Choices for Off-site Machines

- 1) Install the Kerberos client (and optionally the Kerberized ssh client) software on your machines and sign up to be part of the FNAL.GOV strengthened realm. This means you can connect to Fermilab computers using the Kerberized version of a network connection program. This is the preferred method if you are able to do this.
- 2) Leave your machines unstrengthened and always log in using your CRYPTOCARD (see Appendix B: *Getting Started with your CRYPTOCARD*). Note that if you choose to do this and you need to perform operations that involve typing your Kerberos password, you must first ensure that your connection is encrypted in order to prevent your password from being exposed. One way to ensure encryption is to use ssh (with encryption option on) to log in to the strengthened machine initially, using your CRYPTOCARD. You must NEVER type in your password if you are on an unencrypted channel! This means that there is no way to perform any Kerberos command that requires a password while logged in using an X-terminal.
- 3) Your site may have its own version of strong authentication which may be acceptable to Fermilab and then you could become a trusted realm.

The Cryptography Publishing Project is making MIT Kerberos V5 release 1.2.1 available for export without restriction (software for Macintosh excepted); see <http://www.crypto-publish.org/>.

If people need to log in from your site to change their passwords, there must be at least one local machine on which there is software which will allow it to be done locally or over an encrypted connection (e.g., Kerberos, ssh, WRQ). The `fnkerb.fnal.gov` system, described in section 5.1 *Trying Out Kerberos on fnkerb.fnal.gov*, is a Kerberized host available for changing passwords. It is accessible to anyone with an account on FNALU.

## 5.9.2 Obtaining CRYPTOCARDS

All users, on-site and off-site, can request a CRYPTOCARD using the *Form to Request Kerberos Principal and/or Related Items* at <http://www.fnal.gov/cd/forms/strongauth.html>. If you visit Fermilab occasionally, come by WH8NE to pick it up when it's ready. For those experimenters or other users who will not be visiting Fermilab,

CRYPTOCards can be mailed. Each group or experiment should have a person designated to mail CRYPTOCards; contact the appropriate person to request mailing.

### 5.9.3 Exporting CRYPTOCards



For users outside the U.S., you can bring a CRYPTOCard back to your home or institution, with no customs problems since the cards are for authentication, not encryption. They can be mailed outside the U.S., too.

### 5.9.4 Network Address Translation



There is an issue concerning users who maintain a small network of computers at home and whose ISP subjects them to NAT (Network Address Translation). Typically, the user dials up with a NAT box or a Linux host configured to do NAT for the house network, and receives one address from his or her ISP. This address may be static or dynamic. In either case, NAT can make it difficult or impossible to authenticate over the network to the FNAL.GOV realm.

There are a couple of solutions, one of which is to keep your home machines unKerberized, and use a CRYPTOCard. If you want to Kerberize your home machines, we would first recommend that you change ISPs to one that eschews NAT. Barring that, you may be able to work around NAT:

- *if* your home machines (Linux or Macintosh) have **kerberos** installed,
- *if* there is a single fixed “public” IP address associated with your machines’ real IP addresses, and the outside world sees this public IP address as the source of packets that come from your machines,
- and *if* you can determine this fixed IP address.

To be able to authenticate, you’d need to include this public IP address in your local `/etc/krb5.conf` file under the `[libdefaults]` section as:  
`proxy_gateway = <fixed.IP.address>`. If the address is dynamic, this solution will rapidly become annoying, no doubt.

### Windows



If you’ve installed **WRQ®** on your Windows system(s), you will not be able to authenticate if your ISP uses NAT. Remove this software from your system(s) and use a CRYPTOCard. The vendor is aware of this problem, and may address it in future releases of the software.

In the meantime, you can use a combination of an ssh client (e.g., F-secure) with Exceed or the Reflection X Manager (but make sure your site is not behind a firewall in addition to NAT).

## Linux

If you install Linux, configure your machine such that its hostname is equivalent to the external hostname your ISP uses, then install a Kerberos client. (If you're not sure how to configure, send an email to [kerberos-users@fnal.gov](mailto:kerberos-users@fnal.gov), or check the archives.)

## Macintosh

To enable **BetterTelnet** to work for a Kerberized Macintosh in a NAT environment, you must add the following line to the `libdefaults` section of the `Kerberos Preferences` file (Note that this reduces the security of Kerberos.):

```
noaddresses = true
```

Forwardable tickets do not work. Opening a connection with **BetterTelnet** results in a dialog box from the Kerberos5 Telnet Plugin about the forwarded credentials being refused due to bad address. Clicking **OK** will result in the telnet connection opening as expected, otherwise.

## 5.10 Troubleshooting your Authentication Problems

---

If you send mail to [kerberos-users@fnal.gov](mailto:kerberos-users@fnal.gov) requesting help in diagnosing a failure, please include: principal name, date, time and IP address from which authentication failed, in addition to the error message and other error-related information.

- If authentication fails, one of four things is likely to be wrong:
  - (1) your password,
  - (2) the date/time on your system (see section 9.1.6 *Synchronize your Machine with Time Server*),
  - (3) the local host name in the `/etc/hosts` file (see section 11.3 *The /etc/hosts File*), or
  - (4) your CRYPTOCARD is not configured for the target realm. The error message doesn't necessarily help you determine the problem: "Preauthentication failed ...", or "Cannot establish a session with Kerberos administrative server..."

For **WRQ** connections, click **HELP** for possible causes. It's usually a realm mismatch, a wrong password, or a system clock error.



- “Incorrect net address” usually refers to NAT or a multiple-IP address host. For WRQ, there is no solution other than to change ISP or WRQ software. For UNIX, edit the `[libdefaults]` in `/etc/krb5.conf`: add `proxy_gateway=<your fixed IP address>`. For Macintosh, edit the `[libdefaults]` in the Kerberos Preferences file: add `noaddresses=true`.
- YP problem: The error “do\_ypcall: clnt\_call: RPC: Timed out” typically indicates a local problem on your system or site network. Your machine is likely using YP (NIS) for host name-to-address resolution and you have a transient problem with your YP server(s).
- When using the Kerberized versions of **telnet**, **rlogin**, or **rsh** (see Appendix D: *Network Programs Available on Kerberized Machines*) to connect to another machine in the strengthened realm, some users have had to use the `-l <login_name>` option even when the login names on both systems match. (Don’t ask why.) You definitely need to use this option if the login names don’t match.
- If another principal has authenticated in your login account, you (the original user) may need to reauthenticate using the `-l <login_name>` option (with your login name).
- It is unlikely that all the KDCs would be down or unreachable at the same time. However, in this situation, if your machine runs the Kerberos login program, your attempt at login with your Kerberos password will fail. You should be able to try again and succeed using your standard UNIX password, but of course you will not be able to access Kerberized services.
- “KDC policy rejects request” or “KDC can’t fulfill requested option” usually means either you’re requesting a forwardable ticket for a `/root` or `/admin` instance (not allowed), or you’re trying to forward a ticket that’s not forwardable, or renew one that’s not renewable.
- “Key version number for principal in key table is incorrect” means either the keytab has changed since the service ticket was obtained (to solve, run **kinit -R** or **kinit**), or the service key (for host principal) in the KDC was changed after the keytab file was created (to solve, recreate keytab file on host, see section 11.8 *Installing Service Host Keys*).
- Cannot contact any KDC for requested realm. Caused by firewall blocking KDC request or reply, or DNS failure.
- “Server not found in Kerberos database” Possible causes include: local hosts file or NIS map giving wrong name for host (check `/etc/hosts` file and make sure the full host name appears first; see section 11.3 *The /etc/hosts File*), or a bad or missing `[domain_realm]` mapping in `/etc/krb5.conf`. It was also a bug in Fermi Kerberos v1\_2; to solve, upgrade.

- Kerberos V5 refuses authentication because telnetd: krb5\_rd\_req failed: > Key version number for principal in key table is incorrect

You probably have a ticket that you acquired before kerberos was installed on the host which has kvno=1, but after installation (and within the life of that ticket) the kvno gets incremented upon keytab creation. Destroy and recreate your tickets.

- aklog: Couldn't get fnal.gov AFS tickets:, aklog: unknown RPC error (-1765328352) while getting AFS tickets

You may have failed to get fresh tickets from your screensaver unlock. A fresh **kinit** should clear this right up.

## SSH Problems

- Some users of Kerberized **ssh** v1\_2\_27 have encountered a harmless but misleading message upon authentication:

```
aklog: can't get afs configuration
(afsconf_Open(/usr/vice/etc))
```

To get rid of this message, add `AFSRunAklog no` to `/etc/ssh_config` and restart **sshd**.

- Logins from Kerberized **ssh** clients to unstrengthened **ssh** servers can fail. This does not happen with the Fermi **ssh**. You can work around this by explicitly using the `-l <login_name>` option even if the login names on both systems match. (Again, don't ask why.)
- If you get prompted for a password when you login from a machine with Kerberized ssh, and you already have valid tickets, check to make sure the following line is in the `[domain_realm]` section of your `/etc/krb5.conf` file:

```
.fnal.gov = FNAL.GOV
```

Kerberized ssh token-passing won't work without it.